

CLAIMS

What is claimed is:

- 1 1. A method for on-access computer virus scanning of files in an efficient  
2 manner, comprising the steps of:
  - 3 (a) identifying a process for accessing files;
  - 4 (b) selecting virus detection actions based at least in part on the process; and
  - 5 (c) performing the virus detection actions on the files.
- 1 2. The method as recited in claim 1, wherein the process is carried out by an  
2 executable file.
- 1 3. The method as recited in claim 1, wherein the virus detection actions are  
2 selected by determining a category associated with the process, and selecting  
3 a set of virus detection actions based on the determined category.
- 1 4. The method as recited in claim 1, and further comprising the steps of  
2 identifying the files being accessed, and selecting the virus detection actions  
3 based at least in part on the identity of the files.
- 1 5. The method as recited in claim 1, wherein the process is identified by  
2 inspecting at least one of a name of the process, a path of the process, a file  
3 signature associated with the process, a version of the process, a  
4 manufacturer of the process, a function being called during the process, an  
5 owner of the process, a name of an executable file associated with the  
6 process, a method in which files are being accessed by the process, type(s) of  
7 shared libraries used by the identified process, and a user of the process.

09585811-053100

- 1 6. The method as recited in claim 1, wherein no virus detection actions are  
2 selected upon the identification of a predetermined process.
- 1 7. A computer program product for on-access computer virus scanning of files  
2 in an efficient manner, comprising:
  - 3 (a) computer code for identifying a process for accessing files;
  - 4 (b) computer code for selecting virus detection actions based at least in part on  
5 the process; and
  - 6 (c) computer code for performing the virus detection actions on the files.
- 1 8. The computer program product as recited in claim 7, wherein the process is  
2 carried out by an executable file.
- 1 9. The computer program product as recited in claim 7, wherein the virus  
2 detection actions are selected by determining a category associated with the  
3 process, and selecting a set of virus detection actions based on the  
4 determined category.
- 1 10. The computer program product as recited in claim 7, and further comprising  
2 computer code for identifying the files being accessed, and selecting the virus  
3 detection actions based at least in part on the identity of the files.
- 1 11. The computer program product as recited in claim 7, wherein the process is  
2 identified by inspecting at least one of a name of the process, a path of the  
3 process, a file signature associated with the process, a version of the process,  
4 a manufacturer of the process, a function being called during the process, an  
5 owner of the process, a name of an executable file associated with the  
6 process, a method in which files are being accessed by the process, type(s) of  
7 shared libraries used by the process, and a user of the process.

09585811-053100

- 1 12. The computer program product as recited in claim 7, wherein no virus  
2 detection actions are selected upon the identification of a predetermined  
3 process.
- 1 13. A system for on-access computer virus scanning of files in an efficient  
2 manner, comprising:  
3 (a) logic for identifying a process for accessing files;  
4 (b) logic for selecting virus detection actions based at least in part on the  
5 process; and  
6 (c) logic for performing the virus detection actions on the files.
- 1 14. The system as recited in claim 13, wherein the process is carried out by an  
2 executable file.
- 1 15. The system as recited in claim 13, wherein the virus detection actions are  
2 selected by determining a category associated with the process, and selecting  
3 a set of virus detection actions based on the determined category.
- 1 16. The system as recited in claim 13, and further comprising logic for  
2 identifying the files being accessed, and selecting the virus detection actions  
3 based at least in part on the identity of the files.
- 1 17. The system as recited in claim 13, wherein the process is identified by  
2 inspecting at least one of a name of the process, a path of the process, a file  
3 signature associated with the process, a version of the process, a  
4 manufacturer of the process, a function being called during the process, an  
5 owner of the process, a name of an executable file associated with the  
6 process, a method in which files are being accessed by the process, type(s) of  
7 shared libraries used by the process, and a user of the process.

- 1 18. The system as recited in claim 13, wherein no virus detection actions are  
2 selected upon the identification of a predetermined process.
- 1 19. A method for on-access computer virus scanning of files of a system in an  
2 efficient manner, comprising the steps of:  
3 (a) identifying a first aspect of the system;  
4 (b) identifying a second aspect of the system;  
5 (c) selecting virus detection actions based at least in part on the first aspect of  
6 the system and at least in part on the second aspect of the system; and  
7 (d) performing the virus detection actions on the files.
- 1 20. The method as recited in claim 19, wherein the first aspect of the system  
2 includes a process adapted for accessing the files, and the second aspect of  
3 the system includes a type of the files.
- 1 21. A computer program product for on-access computer virus scanning of files  
2 of a system in an efficient manner, comprising:  
3 (a) computer code for identifying a first aspect of the system;  
4 (b) computer code for identifying a second aspect of the system;  
5 (c) computer code for selecting virus detection actions based at least in part on  
6 the first aspect of the system and at least in part on the second aspect of the  
7 system; and  
8 (d) computer code for performing the virus detection actions on the files.

Add  
a1

Add  
B1

Add  
C1